J. Symbolic Computation (2001) **31**, 243–257
doi:10.1006/jsco.2000.1017
Available online at http://www.idealibrary.com on IDEAL®

A New Approach to Primary Decomposition

ALAIN SAUSSE*

INRIA-Sophia Antipolis, SAFIR Project, 2004 Route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex, France

The first purpose of this paper is to describe a new mathematical approach for the computation of an irredundant primary decomposition of a given polynomial ideal I. This presentation will be formed of three parts: a decomposition of the associated radical ideal $\sqrt{I}$ to an intersection of prime ideals P_i, then the determination of ideals I_i whose radical is prime (equal to P_i), and finally, the extraction of the possible embedded components included in I_i.

The second is to give an implementation of this algorithm via a new software component, called *The Central Control*†, in which we implemented distributed algorithms performing the basic operations of algebraic geometry.

1. Introduction

Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring, and let $I = \langle f_1, \ldots, f_s \rangle \subset R$ be an ideal and I define an affine variety $V \subset k^n$. The purpose of this paper is to give an algorithm for finding the primary components of V, which is the same problem as finding a primary decomposition for the ideal I, and to describe an implementation using a new software component, called *The Central Control* (see Dalmas *et al.*, 1995 for further details). In our case, the Central Control will allow us to use several cooperating systems and write distributed algorithms.

This work has been strongly influenced by the work of Bayer *et al.* (1990), by the work of Shimoyama and Yokoyama (1995), and by that of Wang (1991). In studying their papers, we sought to rework their methods so as to avoid an induction on the number of variables, and to avoid producing extraneous primary components which would have to be subsequently removed.

Algorithms for primary decomposition in polynomial rings over $\mathbb{Z}$, have been presented by Seidenberg (1978) and Ayoub (1982). Seidenberg was able to present a simplified construction when the base ring was a field, by reducing the problem to zero-dimensional ideals. In the more general cases when the base ring was the integers, he was forced to give a more indirect construction involving first computing all the associated primes, and then isolating the primary component associated with each prime. Ayoub attempted to generalize her construction for fields to principal ideal domains. She

*E-mail: alain.sausse@sophia.inria.fr
†Developed inside the PoSSo European project.

0747–7171/01/010243 + 15 $35.00/0

presented an algorithm which proceeded by induction on the number of variables in the polynomial ring, rather than on the dimension of auxiliary ideals at each stage of the process.

We base our construction on the Gröbner basis algorithm, a very powerful tool in computational ring theory (see Buchberger, 1987). This method allows the solution of systems of polynomial equations. It provides a canonical (relative to a monomial order) set of generators for an ideal which facilitates the execution of basic geometric algebraic operations. Lazard (1985) has also exploited the structure of a Gröbner basis to give a very efficient primary decomposition algorithm for the special case of polynomial rings in two variables over fields.

Gianni *et al.* (1988) proposed a construction of the primary decomposition based on an induction of the dimension which generalizes the one presented by Seidenberg for the field case.

Various researchers have proposed alternatives for certain steps considered here. For example, Eisenbud and Huneke (1992) computed radicals of ideals via an *Ext* group, then the localization by these prime components determine a primary decomposition. They found in a few examples that this approach can be faster. So, in order to take these improvements into account and because our implementation will strongly depend on the efficiency of some existing implementation steps, we shall propose a modifiable and extensible algorithm.

Adequate, readily available implementations have lagged behind the research in this problem area. One technique (Gianni *et al.*, 1988) has been implemented by its authors on the *Axiom* computer algebra system. Grabe (1993) proposed a package available under the *Reduce* computer algebra system with an efficiency depending on the number of indeterminates of the given ideal.

Nevertheless, each operation required to perform a primary decomposition is separately available, and in addition there exists an efficient implementation of each, on existing computer algebra systems. For example, the factorization implementation is efficient in the *Maple* system, and the computation of Gröbner basis is implemented efficiently in the *GB* (Faugère, 1994) system.

We shall propose a cooperation between these systems to form a computing environment. To connect them, we defined and implemented a software component (called "The Central Control") with which it is easy to write an algorithm that distributes the operations on this network of systems. The Central Control is a software component designed to be the kernel of environments for scientific computation and offers common and concurrent access to many tools needed by the scientist and engineer. The Central Control (often abbreviated to CC in the following) communicates with servers that can be general purpose or specialized computer algebra systems, numerical systems, visualization programs, or graphical interfaces. The Central Control abstracts the syntax and semantic differences of the systems so that, for example, an expression computed by *Mathematica* can be used as input to *Maple*.

In the first section we shall introduce our notation and recall the known properties of primary decomposition. Then, we will show the different steps of our approach and develop our fundamental constructions which will enable us to avoid the extraneous components. The second section will present our implementation via a distributed architecture which allows us to implement distributed algorithms. A third section gives a set of primary decomposition computations in both cases where embedded components exist or not.

2. The Primary Decomposition

Why would anyone want to compute a primary decomposition? Computationally, there are at least two good reasons for doing so. First, a basic purpose of a Gröbner basis system is to describe its incoming data to the user. Dimension and geometrical degree are two fundamental invariants easily obtained from a single Gröbner basis computation. To be able to say, "there are components of such and such dimensions, degrees, and multiplicities, and they are nested as follows," would be considerably more useful. Second, many constructions involving families of varieties require, or make the most sense, when the variety (associated to the given ideal I) is irreducible. Computing the flattening stratification of a family of varieties is a prototypical example of such a construction.

2.1. NOTATIONS

Let k be a field. We note $k[x_1, \ldots, x_n] = R$, the polynomial ring in n variables with coefficients in k. Let $I \subset R$ be an ideal. I is defined by its generators which are polynomials:

$$I = \langle f_1, \ldots, f_s \rangle \qquad \text{with} \qquad f_i \in k[x_1, \ldots, x_n]$$

where I defines an affine variety $V \subset k^n$.

2.2. MINIMALITY AND UNICITY

As is well known, embedded primary components are not uniquely determined. Moreover, the information contained in any particular choice is arbitrary. For example, suppose that $I = Q_1 \cap Q_2$ is a primary decomposition, with associated primes $P_1 \subset P_2$. Then the corresponding variety V can be written as a union $V_1 \cup V_2$ with V_2 as an embedded primary component of V with support contained in V_1. In this case, the quotient Q_1/I is uniquely defined, but Q_2 may be replaced by any P_2-primary ideal having the same intersection with Q_1. Geometrically, V_2 is like an iceberg: we can see the portion protruding out of V_1, represented by the quotient Q_1/I, but we cannot see the non-canonical, "submerged" portion, which could have any shape whatsoever.

This behavior is revealed in even the simplest examples of a primary decomposition: $I = \langle x^2, xy \rangle \subset k[x, y]$ can be decomposed as $I = \langle x \rangle \cap \langle x^2, y \rangle$, or more generally as $I = \langle x \rangle \cap \langle x^2, xy, y^d \rangle$, for any $d \geq 1$. In this example, V is a line with an embedded point, and the various choices for the embedded point V_2 differ in the multiplicity d of their intersections with the line V_1.

2.3. AN OVERVIEW OF THE ALGORITHM

As in Shimoyama and Yokoyama (1995), we chose to define and divide our approach to three intermediate steps. The first one is to determine a prime decomposition of the radical ideal $\sqrt{I}$ via the "Characteristic Set" method (Wang, 1991) based on that of Ritt–Wu. Therefore $\sqrt{I} = P_1 \cap \cdots \cap P_r$. Then, we use an original method of localization to isolate the components whose corresponding ideals I_j, $j = 1 \cdot r$, have prime radicals (equal to P_j). We can also have embedded primary components. The last step is to define and use an extraction method using the flatness notion which is based on the study of fibers of a surjective projection, in order to find the primary components Q'_j with a maximal dimension m_j. It remains to find from the associated primes and via the normal cone theory, the primary decomposition of components with a lower dimension.

2.4. MATHEMATICAL FOUNDATIONS

DEFINITION 2.1. An ideal I in $k[x_1, \ldots, x_n]$ is primary if $fg \in I$ implies either $f \in I$, or $g^m \in I$ for some $m > 0$.

LEMMA 2.1. *If I is primary, then $\sqrt{I}$ is prime and is the smallest prime ideal containing I.*

DEFINITION 2.2. If I is primary and $P = \sqrt{I}$, then we say that I is P-primary.

THEOREM 2.1. *Every ideal $I \subset k[x_1, \ldots, x_n]$ can be written as a finite intersection of primary ideals.*

DEFINITION 2.3. Let $I = \cap_{i=1}^{r} Q_i$ be an primary decomposition of an ideal I. This decomposition is called minimal or irredundant if the $\sqrt{Q_i}$ are all distinct and $Q_i \not\supset \cap_{j \neq i} Q_j$.

Noether tells us that the radicals of ideals in a minimal decomposition are uniquely determined.

LEMMA 2.2. *Let Q be a P-primary ideal (that is, $\sqrt{Q} = P$), and $f \in R$. Then:*

(i) if $f \in Q$ then $(Q : f) = R$;
(ii) if $f \notin P$ then $(Q : f) = Q$;
(iii) if $f \in P$, $f \notin Q$, then $(Q : f)$ is P-primary.

THEOREM 2.2. *Let $I = \cap_{i=1}^{r} Q_i$ be a minimal primary decomposition of a non-trivial radical $I \subset k[x_1, \ldots, x_n]$. Then the Q_i are prime and are the ones occurring in the set: $\{(I : f)$ with $f \in k[x_1, \ldots, x_n]\}$.*

So, if $\sqrt{I} = \cap_i P_i$, then we have $(\sqrt{I} : f^\infty) = \bigcap_i (P_i : f^\infty) = \bigcap_{f \notin P_i} P_i$. In particular, if $f \notin P_1$ and $f \in P_j$ for all $j \neq 1$, then $(\sqrt{I} : f^\infty) = P_1$.

DEFINITION 2.4. Let I be an ideal in $k[x_1, \ldots, x_n]$. A primary component Q_i of I is called an isolated primary component if its associated prime $\sqrt{Q_i}$ is a prime component of $\sqrt{I}$.

Otherwise, it is called an embedded primary component, and its associated prime is called an embedded prime.

In accordance with Theorem 2.2, our first step consists of computing the prime decomposition of the associated radical with I.

2.5. IRREDUCIBLE VARIETY DECOMPOSITION

THEOREM 2.3. *If k is an algebraically closed field, then every radical ideal of $k[x_1, \ldots, x_n]$ can be written as a finite intersection of prime ideals $I = P_1 \cap \cdots \cap P_r$, where $P_i \not\subset P_j$ for $i \neq j$.*

EXAMPLE. $I = \langle xz - y^2, x^3 - yz\rangle$. I is a radical ideal. We remark that $\mathbf{V}(x, y) \subset \mathbf{V}(I)$. Hence $I = \langle x, y\rangle \cap (I : \langle x, y\rangle)$ with $(I : \langle x, y\rangle) = \langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = (I : \langle x\rangle)$. Thus, $I = \langle x, y\rangle \cap (I : \langle x\rangle)$. To represent $\langle x, y\rangle$ as a quotient ideal of I, let us think geometrically. The idea is to remove W from V. Of the three equations defining W, the first two give V. So it makes sense to use the third one, and we can check that $(I : \langle x^2y - z^2\rangle) = \langle x, y\rangle$. It remains to show that $(I : \langle x\rangle)$ and $(I : \langle x^2y - z^2\rangle)$ are prime ideals.

To implement this concept of prime decomposition in irreducible varieties, we used a library that uses the *Characteristic Set* method and allows for the computation of a prime decomposition of the associated radical ideal to the given ideal according to Theorem 2.3. This library has been developed by Dongming Wang, and is available under the *Maple* system.

2.6. LOCALIZATION METHOD

DEFINITION 2.5. Let I be an ideal of $R = k[x_1, \ldots, x_n]$ and T a multiplicatively closed set in R. We denote the set $\{a \in R \mid \exists\ b \in T\backslash\{0\},\ \ ab \in I\}$ by $IR_T \cap R$, and call it the localization of I with respect to T. For a finite set S in R, we denote by (S) the multiplicatively closed set generated by S. For the multiplicatively closed set $R\backslash P$, where P is a prime ideal, we simply denote $IR_P \cap R$ the localization of I with respect to $R\backslash P$.

LEMMA 2.3. *Let I be an ideal of R and f be an element in R. Then, there is an integer k such that $(I : f^k) = IR_{(f)} \cap R = (I : f^\infty)$. Moreover, in this case, $I = (I : f^k) \cap \langle I, f^k\rangle$.*

Geometrical meaning: by this lemma, we separate the components (viewed with their multiplicities) to two families: one consisting of components that are not contained in a multiple of the hypersurface $f = 0$, and defined by $(I : f^k)$, and the other consisting of components that are contained in a multiple of the hypersurface $f = 0$ with extraneous components coming from the intersection (whether it exists) with this hypersurface and the first family.

PROPOSITION 2.1. *Let $I \subset R = k[x_1, \ldots, x_n]$ be, $P = \{P_1, \ldots, P_m\}$ be the set of associated primes of I, and $P_{iso} = \{P_1, \ldots, P_r\}$ be the set of isolated primes of I (that is the set of prime components of $\sqrt{I}$), where $1 < r \leq m$. Moreover, let $Q = \{Q_1, \ldots, Q_m\}$ be a primary decomposition of I. For each i, $i = 1, \ldots, r$, suppose that S_i is a finite set in R which satisfies to the conditions $S_i \cap P_i = \emptyset$, and $S_i \cap P_j \neq \emptyset$ for $i \neq j$. Then:*

- *the ideal $IR_{(S_i)} \cap R$ has a prime radical P_i,*
- *the set $\mathcal{Q}_i = \{\mathcal{Q} \in Q \mid \mathcal{Q} \cap S_i = \emptyset\}$ gives a primary decomposition of $IR_{(S_i)} \cap R$, that is, $IR_{(S_i)} \cap R = \bigcap_{\mathcal{Q} \in \mathcal{Q}_i} \mathcal{Q}$.*

PROOF. Let $S_i = \{u_1, \ldots, u_a\}$ be the set such that $\forall j \neq i$, $\exists\ u_l$ with $u_l \notin P_i$ and $u_l \in P_j$, for $1 \leq l \leq a$. By Lemma 2.3, we can write $IR_{(S_i)} \cap R = ((I : {u_1}^\infty) : \ldots : {u_l}^\infty)$. From a geometrical point of view, if $u_1 \in P_1$, which is equivalent to $\mathbf{V}(P_1) \subset \mathbf{V}(u_1)$, then:

$$\mathbf{V}(I : {u_1}^\infty) = \mathbf{V}(I) \text{minus the components inside } \mathbf{V}(u_1) \text{ and in particular, minus the ones of } P_1.$$

Now, if $u_1 \notin P_i$ then the components of $\mathbf{V}(P_i)$ remain. Hence $\mathbf{V}(IR_{(S_i)} \cap R) = \mathbf{V}(P_i)$. Let us show the second point by an idealistic approach. Let $I = \cap_{i=1}^{m} Q_i$ be a primary decomposition of I associated to P. Show this $\forall u_l,\ u_l \notin Q$. We get $(I : {u_1}^\infty) = \bigcap(Q_i : {u_1}^\infty) = \bigcap_{u_1 \notin Q_i} Q_i$. In the same way $((I : {u_1}^\infty) : {u_2}^\infty) = \underbrace{\bigcap_{u_2 \notin Q_i} \bigcap_{u_1 \notin Q_i} Q_i}_{(u_1,u_2) \cap Q_i = 0}$, and so on. Hence the set $\mathcal{Q}_i$ gives a primary decomposition of $IR_{(S_i)} \cap R$. □

Now, we must compute these isolators $S_1, \ldots, S_r$. So after an iterated quotient computation, we will be able to considerate each isolated component I_i of I.

PROPOSITION 2.2. *If k has more of r elements (for example infinite), then we can choose $t_1, \ldots, t_r \in k[x_1, \ldots, x_n]$ such that $t_j \notin P_i$ if $j \neq i$, and $t_j \in P_j$. Thus*

$$\forall i,\ S_i = \{t_1, \ldots, \widehat{t_i}, \ldots, t_r\}$$

satisfies the conditions of Proposition 2.1.

PROOF. Fix $j = 1$ to simplify this proof.

$\forall i \neq 1$, $P_1 \not\subset P_i$ hence $\exists\ u_i \in P_1$ et $u_i \notin P_i$. We search by recurrence over i, for $i = 2 \ldots r$, $v_i = a_2^i u_2 + \cdots + a_r^i u_r$, $a_l^i \in k$ such that $v_i \in P_1$ and $v_i \notin P_l$, $2 \leq l \leq i$. If $i = 2$, we take $v_2 = u_2$. Suppose v_i and consider $v_{i+1} = av_i + bu_{i+1}$. $\forall a, b$, $v_{i+1} \in P_1$, and if $v_i \notin P_{i+1}$ we take $b = 0$ and it is complete. If $v_i \in P_{i+1}$, we take $b = 1$ and so $v_{i+1} \notin P_{i+1}$. It remains to choose a in order that $v_{i+1} \notin P_2, \ldots, P_i$. However, we remark that if for some value of a, $av_i + u_{i+1} \in P_l$ then $\forall a' \neq a$ we have $a'v_i + u_{i+1} = (a' - a)v_i + (av_i + u_{i+1}) \notin P_l$. Hence it suffices to test at most $i - 1$ values of a to find one such that $av_i + u_{i+1} \notin P_l$ for $l = 2, \ldots, i$. Finally, we note $t_1 = v_r$. Then, it remains to iterate this process for $j = 2, \ldots, r$. □

This proof gives us a constructive way to compute the sets S_i. With Proposition 2.2 and taking $s_i = \mathrm{lcm}(S_i)$, we get

$$(I : {s_i}^\infty) = (((((I : {t_1}^\infty) : {t_2}^\infty) : \ldots : {t_{i-1}}^\infty) : {t_{i+1}}^\infty) : \ldots : {t_r}^\infty) = I_i$$

where I_i is an ideal with a prime radical.

By applying Lemma 2.3, we get the following decomposition of I: $I = I_1 \cap \cdots \cap I_r \cap J$ where J is not uniquely defined, and I_i is as above. We can take as ideal J the ideal $J_1 = \langle I, s_1^{k_1}, \ldots, s_n^{k_n} \rangle$. But the components of J are divided to extraneous components which will disappear with an irredundant decomposition of I (expensive operation), and, embedded components of I corresponding to subvarieties included in intersections of two hypersurfaces $\{t_i = 0\}$, $\{t_j = 0\}$, which would have been forgotten in the previous separation process. So, we propose (and that is very different from Shimoyama and Yokoyama (1995)) to compute J by $J = (I : (I_1 \cap I_2 \cap \cdots \cap I_r))$. In this case, the primary components of J are embedded primary components of I which are not components of I_i. It thus remains to recall the general program by substituting I for J to get, at the end of this recurrence, a decomposition of I in ideals I_i with prime radical.

2.7. AN EXTRACTION METHOD

We must now extract the embedded components of components I_i with a prime radical.

We chose a geometrical presentation. Our method consists first of studying a projection, then studying the fiber projection in order to detect possible embedded components. For that, we define a flattener in relation to a projection, then we connect this object to the flatness notion of a morphism. A quotient computation allows us to then find the component of I_i with the maximal dimension, called $top(I_i)$. Finally, to compute a primary decomposition of I_i, we determine a power of each associated prime that geometrically contains a part of its primary component.

2.7.1. MATHEMATICAL BASES

The proofs of theorems, propositions and lemmas, can be found in Sausse (1995).

DEFINITION 2.6. Let $W \subset V \subset k^n$ be affine varieties. Denote the affine coordinate ring of V by R, and suppose that the ideal of W in V is $I \subset R$. The blowup of V along W is defined by $Bl_W V = Proj(R \oplus I \oplus I^2 \oplus \ldots) = Proj(R[It])$, and the normal cone of W in V is $N_W V = Proj(R/I \oplus I/I^2 \oplus \ldots) = Proj(R[It] \otimes_R R/I)$, where $R[It] \subset R[t]$ for a new variable t.

The inclusion $R \subset R[It]$ induces a surjection of varieties $\pi : Bl_W V \to V$, and $N_W V \to W$.

PROPOSITION 2.3. *Let $R = k[x]/J$ be a ring. Let $I = \langle f_1, \ldots, f_m \rangle \subset k[x]$ be an ideal. If W and V are defined as above then $Bl_W V = Proj(k[x,y]/L)$ and $N_W V = Proj(k[x,y]/(L+I))$, where $L = \langle J, y_1 - tf_1, \ldots, y_m - tf_m \rangle \cap k[x,y]$ for a new variable t.*

EXAMPLE. Our main application of normal cones will be in the case where V is not reduced. Let $P \subset k[x]$ be a prime ideal, and let $Q \subset P$ be a P-primary ideal. Let $V = \mathbf{V}(Q)$ and $W = \mathbf{V}(P)$. Thus $W \subset V$. Let $N_W V = Proj(A)$ be where $R = k[x]/Q$, $I = P\,R$ and A is the graded ring $R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \ldots$ Let l be the smaller integer such that $P^l \subset Q$. Then $I^l = 0$ and $A = R/I \oplus \cdots \oplus I^{l-1}/I^l$. Thus, for $d \geq l$ $A_d = 0$. Geometrically, this means that the homogeneous ideal $k[y]$ of each fiber of the map $\pi : N_W V \to W$ is primary in relation to the maximal ideal.

We suppose now that W is reduced and irreducible, that is, $R = k[x]/I \cap k[x]$ does not have divisors of zero.

Let $I \subset S = k[x,y]$ be an ideal. Consider the projection π from k^n to k^m:

$$\begin{array}{rcl} \mathbf{V}(I) = V & \subset & k^n \\ \pi \downarrow & & \downarrow \\ \mathbf{V}(I \cap k[x]) = W & \subset & k^m \end{array}$$

The projection π can be thought of as a family of ideals (or varieties) parametrized by W. If $p \in W$, the corresponding ideal is $I(p) = \{f(p) | f \in I\} \subset k[y]$.

DEFINITION 2.7. Let $>_1$ be any multiplicative order on the monomials of $k[y]$, and $>_2$ a multiplicative order on $k[x]$. Then, we define the product order $>$ by:

$$x^B y^A > x^D y^C \Leftrightarrow \begin{cases} \text{either} & y^A >_1 y^C, \\ \text{or} & y^A = y^C \text{ et } x^B >_2 x^D. \end{cases}$$

Definition 2.8. Let $I \subset k[x,y]$ be an ideal, and $>$ be the product order (see Definition 2.7). The generic initial ideal of I relative to $>$ is the monomial ideal of $k[y]$ defined by $in_y(I) = \{y^A \mid \exists\, f = \alpha(x)y^A + \cdots \in I, \alpha \notin L\}$ where $L = I \cap k[x]$.

If K is the quotient field of the integral domain R, a Gröbner basis of $IK[y]$ can be written down immediately from a Gröbner basis of I:

Proposition 2.4. *Let $g_j = \alpha_j(x)y^{A_j} + \ldots$, $1 \leq j \leq r$ and $h_j = h_j(x) \in L$, $1 \leq j \leq s$. If $G = \{g_1, \ldots, g_r, h_1, \ldots, h_s\}$ is a reduced Gröbner basis of I with respect to $>$, then $G = \{g_1, \ldots, g_r\}$ is a Gröbner basis for $I^e = IK[y]$, and $in(I^e) = in_y(I)$.*

If $\{y^{A_1}, \ldots, y^{A_p}\}$ minimally generates the monomial ideal $\{y^{A_1}, \ldots, y^{A_r}\}$, then the subset $\{g_1, .., g_p\}$ is a minimal Gröbner basis of I^e. This ideal I^e corresponds to the generic fiber of π. This suggests that for almost every $p \in W$, the Gröbner basis for I specializes to a Gröbner basis of $I(p)$.

Lemma 2.4. *Fix a monomial order $>$ on $k[y]$ and extend it to a product order on $k[x,y]$. Let $h \in k[x]$ be such that $h \notin L$. The following two statements are equivalent:*

(a) whenever $p \in W$ satisfies $h(p) \neq 0$, then $in(I(p)) = in_y(I)$,
(b) for every $y^A \in in_y(I)$, it exists $f \in I$, and an integer N such that $f = h^N y^A + \cdots$

h is called a flattener of π.

The following proposition relates the flattener to components of I. Recall that K is the quotient field of the integral domain R.

Proposition 2.5. *If $h \in k[x]$ is a flattener of I, then*

$$IK[y] \cap k[x,y] = (I : h^\infty).$$

Definition 2.9. (Flatness) Flatness is an algebraic geometric property of a morphism between algebraic varieties which ensures that the fibers fit into a suitably "nice" family. If M is a R-module, M is called R-plat if and only if for every ideal $a \subset R$ (finitely generated), the multiplication map $a \bigotimes_R M \to M$ is injective.

Recall that $R = k[x]/I \cap k[x]$ an integral domain, and $M = k[x,y]/I$ a R-module (not necessarily finitely generated). The following proposition is the key relating flatness to the components of V.

Proposition 2.6. (Algebraic version) *If M is R-plat then for each primary component Q of I, $\sqrt{Q} \cap R = \langle 0 \rangle$.*

(Geometrical version) If $\pi : V \to W$ is flat (that is M is R-plat) with W reduced and irreducible, then each component of V (including embedded components) has a surjective projection on W.

That is, every component of M, including embedded components, dominates W. The geometrical meaning is that if $\pi : V \to W$ is a flat morphism of affine varieties, where W

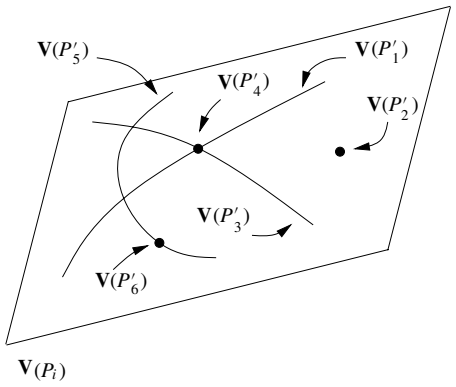

Figure 1. An ideal R_i with its embedded components.

is reduced and irreducible, then each component of V, including embedded components, dominates W.

Definition 2.10. Let $I \subset S = k[x, y]$ be an ideal, and $I = Q_1 \cap \cdots \cap Q_r$ be its irredundant primary decomposition, where each Q_i is a primary ideal. This decomposition is not unique if I has embedded components. Define $top_m(I) = \bigcap_i \{Q_i | dimS/Q_i \geq m\}$. If $dimS/I = d$, then we denote $top_d(I)$ by $top(I)$.

Our method to compute the component of I with the maximal dimension, consists of choosing a projection of V on k^m such that every component of I of dimension of at least m dominates (that is, has a surjective projection on) k^m. By using Gröbner basis and flatness, we can locate those components of V which do not dominate (that is, the embedded components with our hypothesis where the ideals have prime radicals). We then remove these lower dimensional components by saturation (an iterated quotient).

2.7.2. application to an ideal with a radical prime

In this case, I_i has only one isolated component denoted Q_i, that is of greater dimension equal to m, and the previous variety W is equal to k^m. Furthermore, there is necessarily a m-plan of coordinates on which this irreducible component has a surjective projection. Thus, the ideal L of Definition 2.8 is $\{0\}$ (the ideal is already in Noether position).

By applying (recursively) the general procedure of primary decomposition with R_i, we get the set of its associated primes P'_j like an inclusion graph. Indeed, consider for example the algebraic variety 1. We thus have

$$P_i \subset P'_1, \quad P_i \subset P'_2, \quad P_i \subset P'_3, \quad P_i \subset P'_5, \quad P'_3 \subset P'_4, \quad P'_1 \subset P'_4, \quad P'_5 \subset P'_6.$$

It remains for us to determine the primary components having for associated primes, the ones of R_i, that is, to find an irredundant primary decomposition of R_i.

Lemma 2.5. *Let $J = Q \cap R$ be a P-primary ideal of $S = k[x_1, \ldots, x_n]$ with $Q = top(J)$ and $dimS/R < dimS/Q$, and Q' a P-primary ideal such that $J \subset Q'$. Then $Q \subset Q'$.*

We search Q'_j the P'_j-primary ideals such that $R_i = \cap_j Q'_j$. We know that l_j exists such that $P_j^{'l_j} \subset Q'_j \subset P'_j$. Then $R_i \subset R_i + P_j^{'l_j} \subset R_i + Q'_j = Q'_j$. Furthermore $R_i \subset R_i + P_j^{'l_j} \subset top(R_i + P_j^{'l_j})$.

However, $R_i + P_j^{'l_j}$ has as associated prime P'_j and eventually embedded primes $P'_k \supset P'_j$. Hence $top(R_i + P_j^{'l_j})$ has only one associated prime P'_j and thus is P'_j-primary. By applying Lemma 2.5, we get $R_i \subset top(R_i + P_j^{'l_j}) \subset Q'_j$. By now taking the intersection on the j, we have $R_i \subset \bigcap_j top(R_i + P_j^{'l_j}) \subset \bigcap_j Q'_j = R_i$. In conclusion, we get the following irredundant primary decomposition for R_i

$$R_i = \bigcap_j top(R_i + P_j^{'l_j}) \qquad 1 \leq j \leq s.$$

We shall now describe a technique to find the l_j for $1 \leq j \leq s$, which is motivated by the example below.

Example. Suppose that $I \subset J \subset S = k[x_0, \ldots, x_n]$ (where S is the graded polynomial ring) are homogeneous ideals, and $P = \langle x_0, \ldots, x_n \rangle$ the maximal homogeneous ideal. Then $J \cap P^e = I \cap P^e$ if and only if $I = J \cap (I + P^e)$, or, if only if $I_l = J_l$ for all $l \geq e$ that is, I and J are identical in the degrees $\geq e$ (same Hilbert polynomial for $l \geq e$). This smaller degree e can be computed by using the Hilbert series: let

$$H_{S/I}(t) = \sum_{l \geq 0} HP_{S/I}(l)t^l, \quad H_{S/J}(t) = \sum_{l \geq 0} HP_{S/J}(l)t^l$$

be respectively the Hilbert series of S/I and S/J. Since J/I has a finite dimension, we can write the Hilbert serie of J/I as a difference of the previous two series, that is

$$H_{J/I}(t) = a_0 t + a_1 t^2 + \cdots + a_{e-1} t^{e-1}$$

for a certain e where $a_{e-1} \neq 0$. This e is clearly the searched for integer. Thus, we see that if J/I is $\langle x_0, \ldots, x_n \rangle$-primary, then the power e is the degree where I is equal to its saturation J.

We want to generalize the idea of this example to other prime ideals. For that, we shall use the normal cones. Let $W \subset U \subset V \subset \mathbb{P}^{n-1}$ projective varieties defined by the ideals $S \supset P \supset J \supset I$ where P is a prime ideal, J/I is a P-primary ideal, and $S = k[x_0, \ldots, x_n]$ (cf. Example 2.7.1).

Both $N_W V$ and $N_W U$ are defined by graded T-algebras A and B, respectively, where $T = S/P$. The inclusion $U \subset V$ induces a surjection of graded T-algebras:

$$A \to B \to 0.$$

Let K be the kernel of this map. K is also a graded T-algebra.

Lemma 2.6. *For each d, $K_d = (J \cap P^d)/((I \cap P^d) + (J \cap P^{d+1}))$, where K_d is the degree d part of K.*

Proposition 2.7. *$K_l = 0$ for all $l \geq e$ if and only if $J \cap P^l = I \cap P^l$ for all $l \geq e$.*

This proposition gives us an algorithm for finding the desired embedded components. Recall that if I and P are both homogeneous ideals, then the graded S/P-algebra, A,

defining the normal cone, is bi-graded: the first (in "x") is induced by the grading on S, and the second is the grading which makes A a graded S/P-algebra.

2.8. OVERVIEW OF THE ALGORITHM

Finally, to resume our approach of the primary decomposition of a polynomial ideal, we present a pseudo algorithm called "*PrimaryDecomposition* algorithm".

PrimaryDecomposition algorithm:
Input: a polynomial ideal $I \subset k[x_1, \ldots, x_n]$
Output: a set of pairs (Q_i, P_i) such that $I = \cap_i Q_i$ with Q_i P_i-primary ideals.

begin
  $res := \{\}$
  if $I \neq \langle 1 \rangle$ **then**
    lst_indets := indeterminates of I
    $Piso := IVD(I, lst\_indets)$
    $(QL, J) := localization(I, Piso)$
    for each $elt \in QL$ **do**
      $(QL', RL) := extraction(elt)$
      if $RL \neq \langle 1 \rangle$ **then**
        $ensP'_j := Ass(RL)$
        $QL'' := embedded\text{-}primary(elt, ensP'_j)$
      fi
      $res := res \cup QL' \cup QL''$
    done
    if $J \neq \langle 1 \rangle$ **then**
      $res := res \cup PrimaryDecomposition(J)$
    fi
  fi
  return res
end

Here the *IVD* function corresponds to the *ivd* function included in "Charsets" package, the function *localization* implements our localization method, the function *extraction* implements our extraction method, and the function *embedded-primary* corresponds to the searching for the power of our embedded primes.

3. Implementation

To implement this algorithm, we used the Central Control, a software component designed to be the kernel, of environments for scientific computation, and which offers a common and concurrent access to many tools (also called computation servers).

3.1. THE CENTRAL CONTROL

Architectures which support the solution of mathematical problems by linking specialized components, are central to the future growth of Computer Algebra.

The CC presented in Dalmas *et al.* (1995) is in fact an extended *Scheme* interpreter. This enables the dynamic configuration of a network of servers to distribute computations using the full power of the Scheme language. The CC also permits the transparent use of different servers (through the virtual server mechanism) to provide a convenient way for an application program to access computer algebra facilities independently of a particular computer algebra system.

Since there is a wide variety of mathematical objects and associated representations, the CC approach is used to avoid any pre-defined meaning on the objects and requests that are exchanged between the CC and the servers. The CC abstracts the syntaxical and semantic differences of the systems so that, for example, an expression computed by *Mathematica* can be used as input to *Maple*.

We used this interpreter and its programming language to implement this algorithm with the following connected computer algebra systems to perform the basic computation requests: *Macaulay* to test the success of some sub-operations, *Maple* for the polynomial arithmetic as well as the package developed by Dongming Wang for the prime decomposition, and *GB* to compute Gröbner basis. So, we developed *AlGeom*, a fairly complete library for computational algebraic geometry which uses these computer algebra systems to perform its computations (intersection, sum, product, radical, quotient, dimension, associated primes etc ...).

3.1.1. A SHORT PRESENTATION

The Central Control is a Scheme interpreter extended with a set of new primitive operations. These operations include launching or connecting to a server, sending a computation request and receiving the answer, dealing with exceptional conditions: interrupting a server or asynchronously requesting information such as memory size or CPU time already spent in the current computation, and translating requests and answers to ensure the faithful transmission (exchange) of data between servers. This is almost entirely implemented in *Scheme*.

We can illustrate some of the previous items with a short CC session. Here is how to create a PARI server, running on the machine `kama`. `pari1` is bound to a new kind of Scheme object, of type `server`.

```
> (define pari1 (server-create-remote "pari" "kama"
                                      "/net/safir/bin/pariserver"))
#<unspecified>
> pari1
#<server service : pari>
```

This server belongs to the `pari` service. A service is an abstraction common to several servers. Services are used for translating requests and results of computations (this mechanism is described below). We can now send a computation request to our newly created server and get the result back.

```
> (server-compute pari1 '(primes 17))
(result "pari" ("seq" 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59))
```

The PARI server interprets the term `(primes 17)` as a request to compute the first 17 prime numbers. The result is a sequence of prime numbers.

`server-batch` is a function similar to `server-compute` except that it returns a *promise* immediately after transmitting the request without waiting for the computation to end in the server. This function allows the user to run a long computation while doing some other activities in the Central Control.

3.1.2. PROMISES

A promise is a mutable Scheme object associated with a computation in progress on a given server. There are primitive functions acting on promises, to retrieve the associated server, to check if the computation is done or to get its result when available. When the value of a promise is available we say that the promise is *realized*. The function `promise-ready?` can be used to test if a promise is realized.

3.1.3. LAZY COMMUNICATION

As the results of the computations can be large, it is desirable to avoid systematically transmitting them to the CC. Therefore the CC associates a *handle* with a result that is stored in a server. Only the request of specific operations on this handle should cause the effective transmission of the associated result. In some cases, the CC even avoids transmitting the data associated with the handle, for example when a subsequent computation is addressed to the server that owns the value of the handle. This notion of lazy communication reduces the time of communication, computation (for transforming mathematical objects to the representation used by the communication protocol) and the memory used in the CC.

3.1.4. TRANSLATING REQUESTS AND RESULTS

As we do not enforce a standard for encoding all mathematical objects, the CC provides a mechanism to translate from the representation used by one server to another. The translations are performed for each `server-compute` or `server-batch` call, based on the service of the server that the request is submitted to. It is possible to set translations for requests as well as for results. Nevertheless, the CC normally uses a lazy translation and results are "tagged" with the name of the service they come from. Sometimes this could avoid unnecessary translations between two servers of the same service exchanging data.

3.1.5. *Algeom*, A LIBRARY FOR COMPUTATIONAL ALGEBRAIC GEOMETRY

For my Ph.D. thesis (Sausse, 1995), I developed *Algeom*, a fairly complete library for computational algebraic geometry. This library uses *Maple*, *Macaulay* and GB to perform its computations.

Through these functionalities, *Algeom* allowed us to implement our distributed algorithm. This library uses non-trivial programming at the Scheme level to mix different

methods with a complicated "heuristic" control, for example, stopping a process when too much time has elapsed and trying something else. The Central Control allows us to exploit some very useful concurrency in these algorithms as well as to use the most efficient server for each subtask.

4. Examples

4.1. ideals without embedded components

Example 1 Let $I = [-y*x*z*t+(-y^2+y)*z^2, (-x^2+x)*t^2-y*x*z*t, ((-y^2+y)*x-y^3+2*y^2-y)*z^3, (y^2-y)*z^2*t+(-y^2+y)*z^3] \subset k[x,y,z,t]$ be a two-dimensional ideal. Its primary decomposition is

$$I = I_1 \cap I_2 \cap I_3 \cap \cdots \cap I_9$$

where $I_1 = [x, y-1]$ is I_1-primary, $I_2 = [x-1, y]$ is I_2-primary, $I_3 = [x, y]$ is I_3-primary, $I_4 = [x+y-1, t-z]$ is I_4-primary, $I_5 = [x-1, z]$ is I_5-primary, $I_6 = [x, z^2]$ is $[x, z]$-primary, $I_7 = [y-1, t]$ is I_7-primary, $I_8 = [y, t^2]$ is $[y, t]$-primary, and $I_9 = [t^3, t^2*z, t*z^2, z^3, z*(t*x+y*z-z), t*(t*x-t+y*z)]$ is $[z, t]$-primary.

Example 2 Let $I = [((y^3+y^2)*x-y^2-y)*z^2, (y+1)*z*t+(-y^3-y^2)*z^2, (x+1)*z*t+(-y^2-y)*z^2, (x^2+x)*t^2+(-y*x-y)*z*t] \subset k[x,y,z,t]$ be a two-dimensional ideal. Its primary decomposition is

$$I = I_1 \cap I_2 \cap \cdots \cap I_7$$

where $I_1 = [x*y-1, y*z-t*x, t*x^2-z]$ is I_1-primary, $I_2 = [x+1, y+1]$ is I_2-primary, $I_3 = [x+1, z]$ is I_3-primary, $I_4 = [x, z]$ is I_4-primary, $I_5 = [y+1, t]$ is I_5-primary, $I_6 = [y, t]$ is I_6-primary and $I_7 = [z^2, t*z, t^2]$ is $[z, t]$-primary.

4.2. ideals with embedded components

Example 1 Let $I = [e^5, a*e^4, a*b*e^3, b^2*e^3, b^2*c*e^2, a*b*c*e^2, a*c^2*e^2, c^3*e^2, c^3*d*e, a*c^2*d*e, a*b*c*d*e, b^2*c*d*e, b^2*d^2*e, a*b*d^2*e, a*d^3*e, d^4*e] \subset k[a,b,c,d,e]$ be a four-dimensional ideal. We get

$$I = I_1 \cap I_2 \cap \cdots \cap I_5$$

where $I_1 = [e]$ is I_1-primary, $I_2 = [e^2, d*e, d^4]$ is $[d, e]$-primary, $I_3 = [e^3, d^2*e, c*e^2, c*d*e, d^4, c^3]$ is $[c, d, e]$-primary, $I_4 = [b^2, c^3, b*c*d*e, b*c*e^2, b*d^2*e, b*e^3, c^2*d*e, c^2*e^2, d^4, d^3*e, e^4]$ is $[b, c, d, e]$-primary and $I_5 = [a, b^2, c^3, d^4, e^5]$ is $[a, b, c, d, e]$-primary.

Example 2 Let $I = [g^7, a*g^6, b*g^5, c*g^4, d*g^3, e*g^2, f*g] \subset k[a,b,c,d,e,f,g]$ be a six-dimensional ideal. We get

$$I = I_1 \cap I_2 \cap \cdots \cap I_7$$

where $I_1 = [g]$ is I_1 primary, $I_2 = [f, g^2]$ is $[f, g]$ primary, $I_3 = [e, f, g^3]$ is $[e, f, g]$ primary, $I_4 = [d, e, f, g^4]$ is $[d, e, f, g]$ primary, $I_5 = [c, d, e, f, g^5]$ is $[c, d, e, f]$ primary, $I_6 = [b, c, d, e, f, g^6]$ is $[b, c, d, e, f, g]$ primary and $I_7 = [a, b, c, d, e, f, g^7]$ is $[a, b, c, d, e, f, g]$ primary.

5. Conclusion

We have presented a new approach for primary decomposition of ideals, using the basic operations of algebraic geometry and a property of projections, the flatness, which ensures the fibers fit into a suitably "nice" family.

Since few operations required to perform a primary decomposition with an efficient implementation are separately available in computer algebra systems, we chose to make these systems cooperate in the same environment with the CC as a kernel. We are able to use the best implementation for a given task in order to get efficiency, and to easily implement a package of distributed algorithms like for *AlGeom*, a package for the basic operations of algebraic geometry.

Even if it is not a clear gain in terms of computation time, an interesting amount of memory could be saved and thus paging activities and the associated performance penalty can be reduced.

References

Ayoub, C. W. (1982). The decomposition theorem for ideals in polynomial rings over a domain. *J. Algebra*, **76**, 99–110.

Bayer, D., Stillman, M., Galligo, A. (1990). *Primary Decompositions*.

Buchberger, B. (1987). Applications of Grobner bases in non-linear computational geometry. *Mathematical Aspects of Scientific Software*, 59–87.

Dalmas, S., Gaëtano, M., Sausse, A. (1995). The central control: an introduction. In *Proceedings of the PoSSo Workshop on Software*.

Eisenbud, D., Huneke, C. (1992). *Direct Methods for Primary Decomposition*, volume 110 of *Inventiones Mathematicae*.

Faugère, J.-C. (1994). Résolution des Systèmes d'Equations Algébriques. Ph.D. Thesis, University of Paris 6.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomials ideals. *J. Symb. Comput.*, **6**.

Grabe, H.-G. (1993). CALI : A REDUCE package for commutative algebra. Universitat Leipzig.

Lazard, D. (1985). Ideal bases and primary decomposition: case of two variables. *J. Symb. Comput.*, **1**, 261–270.

Sausse, A. (1995). Architecture logicielle distribuée pour le calcul formel. Application à la Décomposition Primaire d'Idéaux. Ph.D. Thesis, University of Nice-Sophia Antipolis.

Seidenberg, A. (1978). Constructions in a polynomial ring over the ring of integer. *Am. J. Math.*, **100**, 685–703.

Shimoyama, T., Yokoyama, K. (1995). *Localization and Primary Decomposition of Polynomial Ideals*, submitted to the JSC.

Wang, D. (1991). A method for determining the finite basis of an ideal from its characteristic set with application to irreductible decomposition of algebraic varieties. Technical Report, RISC.

Originally Received 5 July 1996
Accepted 26 January 2000